Spread Codes and Spread Decoding in Network Coding

Felice Manganiello, Elisa Gorla and Joachim Rosenthal
Mathematics Institute
University of Zurich
Winterthurerstr 190
CH-8057 Zurich, Switzerland
www.math.uzh.ch/aa

***Abstract*— In this paper we introduce the class of *Spread Codes* for the use in random network coding. Spread Codes are based on the construction of spreads in finite projective geometry. The major contribution of the paper is an efficient decoding algorithm of spread codes up to half the minimum distance.**

I. Introduction

In [KK07] Kötter and Kschischang develop a novel framework for random network coding. In this framework information is encoded in subspaces of a given ambient space over a finite field. A natural metric is introduced where two subspaces are 'close to each other' as soon as their dimension of intersection is large. This new framework poses new challenges to design new codes with large distances and to come up with efficient decoding algorithms. Several new papers have been written on the topic and we mention [SKK07] and [MU07].

In this paper we study the class of spreads from finite projective geometry (see e.g. [Hir98]) for possible use in network coding theory. A spread $\mathcal{S}$ is a partition of a vector space by subspaces of a fixed dimension. Elements of a spread are subspaces of a fixed vector space $\mathbb{F}_q^n$ which pairwise only intersect in the origin. The codewords derived in this way are all subspaces of the same dimension. In other words the spread $\mathcal{S}$ is a subset of the finite Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$ consisting of all k-dimensional subspaces in $\mathbb{F}_q^n$. We will call the obtained code a *Spread code*. Since two different elements of $\mathcal{S}$ only intersect in the origin the spread code $\mathcal{S}$ has maximal possible distance among all subsets of $\mathrm{G}(k, \mathbb{F}_q^n)$.

The paper is structured as follows. In the next section we will explain the construction of spreads and we derive some basic properties. In Section 3 the main results of the paper are given. We provide an efficient decoding algorithm for spread codes essentially 'up to half the minimum distance' with its complexity. The decoding algorithm requires methods from linear algebra and the application of the Euclidean algorithm.

II. Algebraic Construction of a Spread Code

Let $\mathbb{F}_q$ be the finite field with q elements. We denote with $\mathrm{G}(k, \mathbb{F}_q^n)$ the Grassmannian of all k-dimensional subspaces of $\mathbb{F}_q^n$. Following [KK07] we define a distance function $d : \mathrm{G}(k, \mathbb{F}_q^n) \times \mathrm{G}(k, \mathbb{F}_q^n) \to \mathbb{Z}_+$ through:

$$\begin{aligned} d(A,B) &:= \dim(A+B) - \dim(A \cap B) \qquad (1)\\ &= \dim(A) + \dim(B) - 2\dim(A \cap B). \end{aligned}$$

It has been observed in [KK07] that $d(A,B)$ satisfies the axioms of a metric on the finite Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$. A constant-dimension code $\mathcal{S} \subset \mathrm{G}(k, \mathbb{F}_q^n)$ has maximal possible minimum distance as long as the intersection of two different codewords of $\mathcal{S}$ is trivial. If two subspaces $A, B \subset \mathbb{F}_q^n$ intersect only in the zero vector then the corresponding subspaces of projective space are nonintersecting. Based on this we will call $A, B \subset \mathbb{F}_q^n$ nonintersecting subspaces as long as they intersect only in the zero vector.

We want to construct an MDS-like code $\mathcal{S} \subset \mathrm{G}(k, \mathbb{F}_q^n)$, i.e. code having maximum possible distance and maximum number of elements. In order to do this we need to restrict our $k, n \in \mathbb{N}$ to some particular cases. It is a well known result that there exists an $\mathcal{S} \subset \mathrm{G}(k, \mathbb{F}_q^n)$ that partitions $\mathbb{F}_q^n$ (i.e. there is no vector in $\mathbb{F}_q^n$ which does not lie in a subspace) and such that any two elements of $\mathcal{S}$ are nonintersecting if and only if k divides n. Those subsets are called *spreads* and this result can be found in [Hir98].

First and third author were partially supported by Swiss National Science Foundation under Grant no. 113251. Second Author was supported by the Forschungskredit of the University of Zurich under Grant no. 57104101 and by the Swiss National Science Foundation under Grant no. 107887.

Consider the case $n = rk$. Let also $p \in \mathbb{F}_q^n[x]$ be an irreducible polynomial of degree k. If we denote with P the $k \times k$ companion matrix of p over $\mathbb{F}_q$, it follows that the $\mathbb{F}_q$-algebra $\mathbb{F}_q[P] \subset \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ is isomorphic to the finite field $\mathbb{F}_{q^k}$. Denoting with $0_k, I_k \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ respectively the zero and the identity matrix and given the above assumptions, we are ready to state the following theorem.

Theorem 1: The collection of subspaces

$$\mathcal{S} := \bigcup_{i=1}^{r} \quad \{\mathrm{rowsp}\,[0_k \ \cdots \ 0_k \ I_k \ A_{i+1} \ \cdots \ A_r] \mid \\ A_{i+1}, \ldots, A_r \in \mathbb{F}_q[P]\} \subset \mathrm{G}(k, \mathbb{F}_q^n)$$

is a spread of $\mathbb{F}_q^n$.

Proof: The cardinality of $\mathcal{S}$ is exactly the maximum number of k-dimensional nonintersecting subspaces of $\mathbb{F}_q^n$, i.e. $\frac{q^n-1}{q^k-1} = q^{k(r-1)} + q^{k(r-2)} + \cdots + q + 1$.

It remains to be shown that any pair of subspaces in $\mathcal{S}$ do only intersect trivially that is equivalent to showing that the $2k \times n$ matrix obtained putting together two matrices generating two different subspaces is full-rank.

We have only two cases. The first where the matrices I_k are not placed at the same column "level". In this case we can find a full-rank submatrix of the form

$$\left[\begin{array}{cc} I_k & A \\ 0_k & I_k \end{array}\right].$$

The second case is when matrices I_k are at the same "level". There exists a submatrix of the form

$$\left[\begin{array}{cc} I_k & A_1 \\ I_k & A_2 \end{array}\right]$$

where $A_1, A_2 \in \mathbb{F}_q[P]$ and $A_1 \neq A_2$. It follows that the determinant of the above matrix is equal to $\det(A_1 - A_2)$ and is nonzero since $A_1 \neq A_2$. ■

Is it possible to find a previous and less general version of this theorem in [CGR07].

Definition 2: Let p be an irreducible polynomial of degree k over $\mathbb{F}_q$. A *spread code* $\mathcal{S}$ is a subset of $\mathrm{G}(k, \mathbb{F}_q^n)$ constructed as in the previous theorem. Following the definition of [KK07] a spread code is a q-ary code of type $[n, k, \log_q\left(\frac{q^n-1}{q^k-1}\right), 2k]$.

Remark 3: Spread codes are related to the Reed-Solomon-like codes over Grasmannians presented in the paper [KK07]. Following the notation of [KK07], let $l = k$ and $m = n - k$. From the construction of Theorem 1, if follows that the subset of $\mathcal{S}$ with $i = 1$ is a subcode of Reed-Solomon-like codes. Moreover, our costruction provides more codewords arising from the cases where $i > 1$.

There is an algebraic geometric way to view the spreads we just introduced. For this identify the set of polynomials in $\mathbb{F}_q[x]$ having degree at most $k-1$ with the field F_{q^k}. Consider the natural isomorphism

$$\begin{array}{rccc} \varphi : & \mathbb{F}_{q^k} & \longrightarrow & \mathbb{F}_q[P] \\ & f & \longmapsto & f(P). \end{array}$$

This isomorphism induces the natural embedding

$$\tilde{\varphi} : \mathrm{G}(l, \mathbb{F}_{q^k}^m) \rightarrow \mathrm{G}(kl, \mathbb{F}_q^{km})$$

with

$$\tilde{\varphi}\left(\mathrm{rowsp}\begin{pmatrix} f_{11} & \ldots & f_{1m} \\ \vdots & & \vdots \\ f_{l1} & \ldots & f_{lm} \end{pmatrix}\right) \\ = \mathrm{rowsp}\begin{pmatrix} f_{11}(P) & \ldots & f_{1m}(P) \\ \vdots & & \vdots \\ f_{l1}(P) & \ldots & f_{lm}(P) \end{pmatrix}.$$

The following theorem is then not difficult to establish.

Theorem 4: If $\mathcal{S} \subset \mathrm{G}(l, \mathbb{F}_{q^k}^m)$ is a spread of $\mathbb{F}_{q^k}^m$ then $\tilde{\varphi}(\mathcal{S}) \subset \mathrm{G}(kl, \mathbb{F}_q^{km})$ is a spread of $\mathbb{F}_q^{km}$.

Clearly $\mathrm{G}(1, \mathbb{F}_{q^k}^r)$ is a spread itself and it therefore follows that the subset defined in Theorem 1 is a spread of $\mathbb{F}_q^n$ as well.

III. Decoding Algorithm

We will continue restricting our study to the case where $n = 2k$ and k is odd. From now on we will consider fixed the irreducible polynomial $p \in \mathbb{F}_q[x]$.

In a first step we want to establish a simple algebraic criterion which characterizes the spread code $\mathcal{S} \subset \mathrm{G}(k, \mathbb{F}_q^{2k})$. For this assume that $C_1, C_2 \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ are matrices such that

$$C := \mathrm{rowsp}[C_1 \ C_2] \in \mathrm{G}(k, \mathbb{F}_q^{2k}).$$

If C_1 is not invertible then $C \in \mathcal{S}$ if and only if $C_1 = 0_k$. If C_1 is invertible then $C \in \mathcal{S}$ if and only if $A := (C_1)^{-1}C_2 \in \mathbb{F}_q[P]$.

We therefore establish a criterion which guarantees that a matrix A is in $\mathbb{F}_q[P]$. Let $\mathbb{F}_{q^k}$ be the splitting field of p over $\mathbb{F}_q$ and $S \in Gl_k(\mathbb{F}_{q^k})$ be an invertible matrix diagonalizing the matrix P, i.e.

$$D := SPS^{-1} = \left[\begin{array}{cccc} \lambda & & & \\ & \lambda^q & & \\ & & \ddots & \\ & & & \lambda^{q^{k-1}} \end{array}\right]$$

where $\lambda \in \mathbb{F}_{q^k}$ is a root of p.

Lemma 5: Let $A \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$. Then $A \in \mathbb{F}_q[P]$ if and only if $AP = PA$.

Proof: If $A \in \mathbb{F}_q[P]$ then clearly $AP = PA$. Assume now $AP = PA$ and $SPS^{-1} = D$. Since the eigenvalues of P are pairwise different and $D(SAS^{-1}) = (SAS^{-1})D$ it follows that SAS^{-1} is a diagonal matrix as well with diagonal entries in $\mathbb{F}_{q^k}$. Let $\{1, \gamma, \dots, \gamma^{k-1}\}$ be a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. One has an expansion:

$$SAS^{-1} = \sum_{i=0}^{k-1} c_i D^i = \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} c_{i,j}\gamma^j D^i$$

with $c_i \in \mathbb{F}_{q^k}$ and $c_{i,j} \in \mathbb{F}_q$.

Equivalently we have:

$$A = \sum_{j=0}^{k-1}\left(\sum_{i=0}^{k-1} c_{i,j}P^i\right)\gamma^j.$$

It follows that $A = \sum_{i=0}^{k-1} c_{i,0}P^i$ and $A \in \mathbb{F}_q[P]$. ■

The following gives an algebraic criterion for checking when a subspace is a codeword.

Corollary 6: The subspace $\mathrm{rowsp}[I_k\ A] \in \mathrm{G}(k, \mathbb{F}_q^{2k})$ is a codeword of $\mathcal{S}$ if and only if SAS^{-1} is a diagonal matrix.

We state now the unique decoding problem. Assume $C := \mathrm{rowsp}[C_1\ C_2] \in \mathcal{S}$ was sent and $R := \mathrm{rowsp}[R_1\ R_2] \in \mathrm{G}(k, \mathbb{F}_q^{2k})$ was received. If

$$\dim(C \cap R) \geq \frac{k+1}{2} \tag{2}$$

then unique decoding is possible. In the sequel we will consider the received subspace $R \in \mathrm{G}(k, \mathbb{F}_q^{2k})$ such that there exists a codeword $C \in \mathcal{S}$ such that (2) holds.

A. Case R_1 not invertible.

Let R and C be subspaces satisfying the condition (2). The goal of this subsection is to analyze the behavior of the decoding problem when R_1 is not invertible.

This situation splits in two different ones. The first one is when $0 \leq \mathrm{rank}(R_1) \leq \frac{k-1}{2}$. The closest codeword in this case is only the subspace $\mathrm{rowsp}[0_k\ I_k]$.

The second case is characterized by $\frac{k+1}{2} \leq \mathrm{rank}(R_1) \leq k-1$. With the following lemma we bring back the decoding problem of the subspace R to the one of a subspace $\tilde{R}$ close related to R and lying in the same ball with center in the codeword C.

Lemma 7: Let $R \in \mathrm{G}(k, \mathbb{F}_q^{2k})$ such that $\frac{k+1}{2} \leq \mathrm{rank}(R_1) \leq k-1$ and $C \in \mathcal{S}$ such that (2) holds. Then there exists a subspace $\tilde{R} := \mathrm{rowsp}[\tilde{R}_1\ \tilde{R}_2] \in \mathrm{G}(k, \mathbb{F}_q^{2k})$ satisfying:

- $\tilde{R}_1$ is invertible,
- $\dim(R \cap \tilde{R}) = \mathrm{rank}(R_1)$, and
- $\dim(C \cap \tilde{R}) \geq \frac{k+1}{2}$.

Proof: Let $t := \mathrm{rank}(R_1)$. Row reducing the matrix $[R_1\ R_2]$ we obtain the matrix $\begin{bmatrix} \bar{R_1} & \bar{R_2} \\ 0 & E \end{bmatrix}$ where $\bar{R_1}, \bar{R_2} \in \mathrm{Mat}_{t\times k}(\mathbb{F}_q)$ with R_1 fullrank and $0, E \in \mathrm{Mat}_{k-t\times k}(\mathbb{F}_q)$ where 0 is the zero matrix.

Since $\mathrm{rowsp}[0\ E] \subset \mathrm{rowsp}[0_k\ I_k]$ we deduce that $\dim(C \cap \mathrm{rowsp}[0\ E]) = 0$. It follows immediately that

$$\dim(C \cap \mathrm{rowsp}[\bar{R_1}\ \bar{R_2}]) = \dim(C \cap \tilde{R}) \geq \frac{k+1}{2}.$$

The matrix representing the subspace $\tilde{R}$ can then be constructed as follows:

- $\tilde{R_1}$ is the completion of the matrix $\bar{R_1}$ to an invertible matrix, and
- $\tilde{R_2}$ is the completion of the $\bar{R_2}$ to a k-square matrix by adding rows of zeros.

■

Corollary 8: The solution to the unique decoding problem for both subspaces R and $\tilde{R}$ consists of the same codeword $C \in \mathcal{S}$.

B. Case R_1 invertible.

We can now construct an algorithm for the unique decoding problem of subspaces with R_1 invertible.

Theorem 9: Let $R := \mathrm{rowsp}[R_1\ R_2] \in \mathrm{G}(k, \mathbb{F}_q^{2k})$ a subspace with R_1 invertible. Then there exists a unique matrix $A \in \mathbb{F}_q[P]$ and a unique matrix $N \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$ of rank at most $\frac{k-1}{2}$ such that

$$R_1^{-1}R_2 = A + N.$$

In this case $\mathrm{rowsp}[I_k\ A]$ is the closest codeword to R in the distance (1).

Proof: The uniqueness follows from the distance properties of the code. Assume $\mathrm{rowsp}[I_k\ A]$ be the closest codeword to R. Since

$$\mathrm{rowsp}\begin{bmatrix} I_k & A \\ R_1 & R_2 \end{bmatrix} = \mathrm{rowsp}\begin{bmatrix} I_k & A \\ 0_k & R_1^{-1}R_2 - A \end{bmatrix}$$

has dimension at most $2k - \frac{k+1}{2} = k + \frac{k-1}{2}$ it follows that the matrix $N := R_1^{-1}R_2 - A$ has rank at most $\frac{k-1}{2}$. ■

Corollary 10: Let $R := \mathrm{rowsp}[R_1\ R_2] \in \mathrm{G}(k, \mathbb{F}_q^{2k})$ a subspace with R_1 invertible. Let $Y := S(R_1^{-1}R_2)S^{-1}$. Then there is a unique polynomial $f \in \mathbb{F}_q[x]$ with $\deg f < k$ such that $Y - f(D)$ has rank at most $\frac{k-1}{2}$.

Proof: The existence follows directly from the last theorem. Concerning the uniqueness assume that $Y = f_1(D) + N_1 = f_2(D) + N_2$. It then follows that

$$R_1^{-1}R_2 = f_1(P) + S^{-1}N_1S = f_2(P) + S^{-1}N_2S$$

and because of the uniqueness part of Theorem 9 the result follows. ■

The algorithm extrapolates the evaluations of the polynomial $f \in \mathbb{F}_q[x]$ from the matrix $Y - f(D)$. Once the polynomial $f \in \mathbb{F}_q[x]$ is found, its evaluation at P gives us the matrix $A \in \mathbb{F}_q[P]$ such that $\mathrm{rowsp}\,[I_k\ A]$ is the codeword closest to R. Notice that the coefficients of f are exactly the coefficients of the expression of $f(\lambda)$ in the basis $\{1, \lambda, \dots, \lambda^{k-1}\}$ of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$.

The following two remarks from finite field theory (see [LN94]) will be important. First, given any $f \in \mathbb{F}_q[x]$ and any $\mu \in \mathbb{F}_{q^k}$, then $f(\mu^q) = f(\mu)^q$. Second, given a finite field $\mathbb{F}_q$ with q elements it holds

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

We outline now the complete decoding algorithm.

Let $R := \mathrm{rowsp}\,[R_1\ R_2]$ be the received subspace satisfying condition (2). Assume that R_1 is invertible. Compute $Y := S(R_1^{-1} R_2) S^{-1}$. If the matrix Y is diagonal, then R is already a codeword of $\mathcal{S}$ by Corollary 6.

Otherwise the matrix $Y - f(D)$ is of the form

$$\begin{pmatrix} y_{1,1} - f(\lambda) & y_{1,2} & \cdots & y_{1,k} \\ y_{2,1} & y_{2,2} - f(\lambda^q) & \cdots & y_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ y_{k,1} & y_{k,2} & \cdots & y_{k,k} - f(\lambda^{q^{k-1}}) \end{pmatrix} =$$

$$\begin{pmatrix} y_{1,1} - f(\lambda) & y_{1,2} & \cdots & y_{1,k} \\ y_{2,1} & y_{2,2} - f(\lambda)^q & \cdots & y_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ y_{k,1} & y_{k,2} & \cdots & y_{k,k} - f(\lambda)^{q^{k-1}} \end{pmatrix}$$

where some entries off of the diagonal are nonzero. Denote by X the matrix obtained from $Y - f(D)$ by substituting x for $f(\lambda)$. By Corollary 10 there exists a unique value for $x \in \mathbb{F}_{q^k}$ (namely $x = f(\lambda)$) such that $\mathrm{rank}(X) \leq \frac{k-1}{2}$. The decoding problem reduces to finding such a value.

The condition on the rank is equivalent to having all minors of size $\frac{k+1}{2}$ of the matrix X being zero. This gives us a system of univariate equations which apriori may be hard to solve. However since the system has a unique solution, every minor is divisible by $(x - f(\lambda))$.

Hence in order to find $f(\lambda)$ it suffices to compute the gcd of the field equation $x^{q^k} - x$ with enough equations from our system. More precisely we look for a nonzero minor of size $\frac{k-1}{2}$ which does not involve any diagonal entry. If no such minor exists, then look for a nonzero minor of smaller size which again does not involve any diagonal entry. Let t be the size of the minor. Complete the corresponding size t submatrix to a submatrix of X of size $\frac{k+1}{2}$. Notice that this can be done by adding $\frac{k+1}{2} - t$ rows and columns with the same index. The determinant of this submatrix is a nonzero polynomial $m \in \mathbb{F}_{q^k}[x]$ which has $f(\lambda)$ as a root.

Apply the Euclidean Algorithm in order to compute

$$g := \gcd(x^{q^k} - x, m).$$

If the degree of g is small, compute its roots and substitute them in X in order to find $f(\lambda)$.

Otherwise compute another minor in the same way as for the previous one. Proceed by computing the gcd of this polynomial with g. The algorithm ends once it finds $f(\lambda)$.

C. *Complexity*

The overall complexity of the algorithm is dominated by the Euclidean Algorithm. In the worst case scenario, i.e. when the maximal nonzero minor off diagonal has size 1, the algorithm's complexity is $\mathcal{O}(q^{k \log_2 3} \log q^k)$ in $\mathbb{F}_{q^k}$.

The complexity could be drastically decreased by the following conjecture: for every error matrix $N \in \mathrm{Mat}_{k \times k}(\mathbb{F}_q)$ of rank $t \leq \frac{k-1}{2}$ there exists a nonzero minor of size t of the matrix X which does not involve any diagonal entry.

Consider now such a nonzero minor of X and extend the related submatrix adding one row and one column with the same index. The determinant of this submatrix leads to an equation of the type $x^{q^i} = \alpha$ with $\alpha \in \mathbb{F}_q$. Raising both sides of the equation to the q^{k-i}-th power and using the field equation of $\mathbb{F}_{q^k}$ we get: $x = \alpha^{q^{k-i}}$. Using the Repeated Squaring Algorithm for computing powers in $\mathbb{F}_{q^k}$, the complexity of the decoding algorithm decreases to $\mathcal{O}(\log q^{k-i}) = \mathcal{O}(k-i)$ operations in $\mathbb{F}_{q^k}$.

A reference for efficient algorithms is [GG03]. In particular see Section 4.3 for the Repeated Squaring Algorithm, Section 11.1 for performing the Euclidean Algorithm, Chapter 14 for factoring univariate polynomials and Section 25.5 for computing determinants.

D. *Non-perfectness of a Spread Code*

Spreads are perfect in the sense that every nonzero vector of $\mathbb{F}_q^n$ is in one and only one subspace of the spread.

In coding theory a code is perfect if the total ambient space is covered with the balls centered in the codewords and having radius half the minimum distance. It arises the question if spread codes are perfect in this sense. The answer turns out to be negative in general and this result can be found in [MZ95].

ACKNOWLEDGMENTS

We would like to thank Joan Josep Climent, Felix Fontein, Verónica Requena and Jens Zumbrägel for many helpful discussions during the preparation of this paper.

REFERENCES

[CGR07] J. J. Climent, F. J. Garcia, and V. Requena. On the construction of bent functions of 2k variables from a primitive polynomial of degree k. preprint, 2007.

[GG03] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[Hir98] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[KK07] R. Koetter and F. Kschischang. Coding for errors and erasures in random network coding. submitted, 2007.

[LN94] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, London, 1994. Revised edition.

[MU07] A. Montanari and R. Urbanke. Coding for network coding. submitted, 2007.

[MZ95] W. J. Martin and X. J. Zhu. Anticodes for the grassman and bilinear forms graphs. *Designs, Codes and Cryptography*, 6(1):73–79, July 1995.

[SKK07] D. Silva, F. Kschischang, and F. Kötter. A rank-metric approach to error control in random network coding. submitted, 2007.